UNITED STATES DISTRICT COURT

FOR THE SOUTHERN DISTRICT OF WEST VIRGINIA

JEDIDIAH WALLS, MICHAEL HILL, AND JENNIFER HILL, individually and on behalf of all others similarly situated, *Plaintiffs*, v. CHARLESTON AREA MEDICAL CENTER, INC., *Defendant*.	No. **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiffs Jedidiah Walls, Michael Hill, and Jennifer Hill, individually and on behalf of all others similarly situated, allege the following complaint against Defendant Charleston Area Medical Center, Inc. ("CAMC" or "Defendant") upon personal knowledge as to their own acts, and based upon their investigation, their counsel's investigation, and information and belief as to all other matters.

SUMMARY OF ACTION

1. This case involves a major data breach exposing private personally identifiable information ("PII") and protected health information ("PHI") for more than 67,000 individuals. As a result of the data, breach Plaintiffs have been directly harmed.

2. CAMC is a large regional medical center comprised of seven hospitals in the Charleston area. It claims to employ more than 8,000 people.[1]

3. On or before October 2, 2024, CAMC was subject to a targeted phishing attack.[2] CAMC alleged that a single CAMC user's email mailbox was compromised as a result of the attack. Although CAMC became aware of the attack on October 2, 2024, it did not or could not terminate the attacker's access until October 3, 2024. Moreover, although CAMC became aware of the breach as early as October 2, 2024, it did not begin notifying impacted patients until February 14, 2025, more than 5 months later.

4. Despite CAMC's claim that only one mailbox was compromised, it appears that at least 67,413 individuals had their personal information exposed as a result of the breach.[3]

5. The compromised information included extremely sensitive personal and health information that criminals could use to commit fraud and identity theft crimes.

6. Members of the Plaintiff class suffered harm in the loss of their private medical and personal information and the extraordinary risk of sale of this data to criminals over the dark web. Even members of the class who have not yet been victims

---

[1] *See* https://www.camc.org/about-camc (Last Accessed February 24, 2025)
[2] *See* https://www.camc.org/sites/default/files/2025-02/2025-02-03%20-%20CAMC%20-%20Substitute%20Notice%20-%204908-3837-5706.1.pdf (Last Accessed February 24, 2025)
[3] *See* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (Last Accessed February 24, 2025)

of identity theft and fraud suffer from significant stress and anxiety about the potential for future harm and have to expend significant time and effort to engage in various services and efforts in the wake of the data breach, including but not limited to examining whether and what PII or PHI has been sold on the dark web, taking measures to protect against identity theft crimes, expenses, and/or time spent on credit monitoring and identity theft insurance, time spent examining bank statements, time spent initiating fraud alerts, and other consequential harms.

7. Plaintiffs, individually and on behalf of a nationwide class allege claims of (1) Negligence, (2) Breach of Implied Contract, (3) Breach of Fiduciary Duty, (4) Invasion of Privacy and (5) seek declaratory and injunctive relief. Plaintiffs ask the Court to compel Defendant to adopt reasonable information security practices to secure the sensitive PII and PHI that Defendant collects and stores in its databases and to grant such other relief as the Court deems just and proper.

PARTIES

Plaintiffs

8. Plaintiff Jedidiah Walls is a resident and citizen of Saint Albans, West Virginia who used Defendant's services. Accordingly, he entrusted Defendant with sensitive PII and PHI. He received a data breach letter from Defendant addressed to himself dated February 14, 2025 advising his personal and health information may have been exposed including but not limited to his first and last name; date of birth; e-mail address; phone number; driver's license; health information, and health insurance information.

9. Plaintiff Michael Hill is a resident and citizen of Kanawha County, West Virginia who used Defendant's services. Accordingly, he entrusted Defendant with

sensitive PII and PHI. He received a data breach letter from Defendant addressed to himself dated February 14, 2025 advising his personal and health information may have been exposed including but not limited to his first and last name; date of birth; e-mail address; phone number; driver's license; health information, and health insurance information.

10. Plaintiff Jennifer Hill is a resident and citizen of Kanawha County, West Virginia who used Defendant's services. Accordingly, she entrusted Defendant with sensitive PII and PHI. She received a data breach letter from Defendant addressed to herself dated February 14, 2025 advising her personal and health information may have been exposed including but not limited to her first and last name; date of birth; e-mail address; phone number; driver's license; health information, and health insurance information.

Defendant

11. Defendant Charleston Area Medical Center, Inc. is a West Virginia corporation with its principal place of business in Charleston WV. It operates seven hospitals: CAMC General Hospital, CAMC Greenbrier Valley Medical Center, CAMC Memorial Hospital, CAMC Plateau Medical Center, CAMC Charleston Surgical Hospital, CAMC Teays Valley Hospital, and CAMC Women and Children's Hospital. It also operates the CAMC Institute for Academic Medicine and the CAMC Foundation.[4]

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction and diversity jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The class contains more

[4] https://www.camc.org/about-camc (Last Accessed February 24, 2025)

than 100 members (indeed, it contains more than 67,000 members), and many of these members have citizenship diverse from Defendant. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the case in controversy.

13. CAMC's data breach notice provided information for putative class members who are citizens of the District of Columbia, Iowa, Maryland, Massachusetts, New Mexico, New York, and North Carolina. On information and belief, a substantial portion of the putative class is comprised of citizens of other states.

14. The exercise of personal jurisdiction over Defendant is appropriate. Defendant's primary place of business is in this District, and it is incorporated in West Virginia.

15. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) because Plaintiffs reside in this district, Defendant conducts substantial business in this District, and Plaintiffs were harmed within this District.

FACTUAL ALLEGATIONS

I. Background:

16. Plaintiffs and members of the Plaintiff Class are former or current patients who used Defendant's services.

17. In order to receive treatment, Plaintiffs and members of the Plaintiff class, provided this non-exclusive list of sensitive PHI and PII as a prerequisite to obtaining healthcare services:

- Full name and mailing or personal address
- State and/or Federal Identification (such as driver's license)

- Health insurance information including but not limited to carrier, policy number, and healthcare card (if applicable)
- Date of birth
- Medical information including but not limited to information about diagnosis and treatment, personal medical history, family medical history, mental health information, information related to STDs and treatment, medication information, and medical record number
- Information about physicians and related medical professionals who had been involved in previous or ongoing treatment of the patient,
- Residence and travel history
- Billing and claims information
- Medicare/Medicaid information including the Medicare patient identifier, Medicare Card, and Medicare Entitlement, Enrollment, and Premium Information
- Information on prescriptions taken including history of taking certain prescriptions.
- Diagnostic results and treatment information
- Information on family members including but not limited to emergency contact information and next of kin
- Personal email addresses and phone numbers
- Other health information and health insurance information

18. The above information is extremely sensitive personal identifying information and personal health information (PII and PHI). This information is

extremely valuable to criminals because it can be used to commit serious identity theft and medical identity theft crimes.

19. Defendant understands the high value of this information. On its website, Defendant states in its Notice of Privacy Practices that it is required to "**Maintain the privacy of your health information.**"[5]

20. As a condition of obtaining Defendant's services, class members entrusted Defendant with this information with the explicit and implicit understanding that the information would be kept secure and that reasonable measures would be taken to maintain and ensure their security, including notification in the event of a breach, commensurate with the value of the data.

II. The Breach

21. At least as early as October 2, 2024, CAMC became aware of the risk of a serious data breach in connection with a targeted phishing attack. This breach impacted more than 67,000 individuals.

22. The sensitivity and scope of the compromised information is significant. Exposed information includes but is not limited to:

- Full name of the patient
- Date of birth
- Email address
- Personal phone number
- Driver's license
- Health insurance information

[5] https://www.camc.org/sites/default/files/2020-11/17-8911.pdf (Last Accessed February 24, 2025)

- Health information[6]

23. This information is extraordinarily sensitive and would be ideal for a criminal agent attempting to commit identity theft or similar crimes against innocent patients. However, no notifications were mailed to the impacted patients for more than four months after the data breach occurred.

24. The fact that name, date of birth, email address, phone number, driver's license information, and health insurance and medical information were all stored in the same place and could be accessed for tens of thousands of patients suggests the existence of a fundamental security flaw and a failure to compartmentalize information and appropriately restrict access to only those with a "need to know." This is especially true considering Defendant has represented that only a single email account was compromised in the breach. A single email account being compromised should not result in the release of highly sensitive personal and medical information for tens of thousands of individuals.

III. Defendant's Prior Conduct

25. This is not Defendant CAMC's first rodeo. CAMC is engaged in an ongoing attempt to settle claims related to a prior data breach which occurred on or about January 2022.

26. The prior data breach is startlingly similar to the present one. In the 2022 data breach, patient data for more than 54,000 individuals was compromised as the result of an email phishing attack. In the prior case, plaintiffs made highly similar

[6] Defendant did not specify in detail what breached "health information" and "health insurance information" means.

claims to those currently at bar including claims of negligence, breach of contract, breach of implied contract, and breach of confidences.[7]

27. Defendant was well aware that the October 2024 breach could occur because it had already been breached in what seems a very similar way in January 2022. Defendant nevertheless did not make sufficient, or potentially any, changes to its security system as a result of the first breach. Defendant knew at all relevant times that it had an obligation to protect and secure the information possessed by Plaintiff and class members, yet it nevertheless failed to adequately secure their PII and PHI.[8]

IV. Defendant Failed to Comply with Reasonable Cybersecurity Standards

28. At all times relevant to this Complaint, Defendant knew or should have known the significance and necessity of safeguarding patients' PII and PHI, and the foreseeable consequences of a data breach. Defendant knew or should have known that because it collected and maintained the PII and PHI for a significant number of patients, a significant number of patients would be harmed by a breach of its systems. Defendant further knew due to the fact that a very similar harm had already occurred as a result of a previous successful phishing attack against Defendant just 3 years ago.

29. Moreover, Defendant significantly and unreasonably delayed in notifying patients about the breach. Although Defendant allegedly learned of the breach on October 2, 2024, it did not begin sending breach notices until February 2025. Not only is this unreasonable delay harmful to patients, but it is particularly egregious because Defendant knows how to do better. In the 2022 data breach, the breach occurred in

[7] https://www.camc.org/sites/default/files/2020-11/17-8911.pdf (Last Accessed)
[8] https://camcdatasettlement.com (Last Accessed February 24, 2025)

January and CAMC sent notices to patients in March.[9] It is unclear why Defendants took twice as long to notify patients as they did the last time they were breached. More than four months is an unreasonable period of time to delay the notification of a data breach of this type.

30. Because PII is so sensitive and cyberattacks have become a rising threat, the FTC has issued numerous guides for businesses holding sensitive PII and emphasized the importance of adequate data security practices. The FTC also stresses that appropriately safeguarding PII held by businesses should be factored into all business-related decision making. Defendant should have been very well-aware of the FTC standards for safeguarding this sensitive information.

31. An FTC Publication titled "Protecting Personal Information: A Guide for Business" lays out fundamental data security principles and standard practices that businesses should implement to protect PII.[10] The guidelines highlight that businesses should (a) protect the personal patient information they collect and store; (b) properly dispose of personal information that is no longer needed; (c) encrypt information stored on its computer networks; (d) understand its network's vulnerabilities; and (e) implement policies to correct security problems.

32. The FTC also recommends businesses use an intrusion detection system, monitor all incoming traffic to the networks for unusual activity, monitor for large amounts of data being transmitted from its systems, and have a response plan prepared in the event of a breach.

---

[9] *Id.*

[10] https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business. (last accessed July 25, 2024)

33. The FTC also recommends that businesses limit access to sensitive PII, require complex passwords to be used on the networks, use industry-tested methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.

34. Businesses that do not comply with the basic protection of sensitive PII are facing enforcement actions brought by the FTC. Failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data is an unfair act or practice prohibited pursuant to Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45.

35. Many states' unfair and deceptive trade practices statutes are similar to the FTC Act, and many states adopt the FTC's interpretations of what constitutes an unfair or deceptive trade practice.

36. Defendant knew or should have known of its obligation to implement appropriate measures to protect its patients' PII but failed to comply with the FTC's basic guidelines and other industry best practices, including the minimum standards set by the National Institute of Standards and Technology Cybersecurity Framework Version 1.1.[11]

37. Defendant's failure to employ reasonable measures to adequately safeguard against unauthorized access to PII constitutes an unfair act or practice as prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45, as well as by state statutory analogs.

38. CAMC was also subject to HIPAA security, breach notification, and privacy standards.

---

[11] https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf. (last accessed July 25, 2024)

39. HIPAA circumscribes security, data privacy responsibilities, and breach-notification obligations designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish standards for electronic transactions and code sets to maintain the privacy and security of protected information.[12]

40. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII and PHI is properly maintained.[13]

41. Defendant is a business associate covered by HIPAA (45 CFR §160.102) and as such is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and the Security Standards for the Protection of Electronic Protected Health Information ("Security Rule"), 45 CFR Part 160 and Part 164, Subparts A and C. They are also required to follow the Breach Notification Rule. 45 CFR Part 160 and Par 164, Subparts A and D.

42. HIPAA requires Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information."[14] HIPAA requires covered entities' business associates to

[12] HIPAA lists 18 types of information that qualify as PHI according to guidance from the department of Health and Human Services Office for Civil Rights, and includes *inter alia*: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.
[13] *See* 45 CFR §164.306 (security standards and general rules); 45 CFR §164.308 (administrative safeguards); 45 CFR §164.310 (physical safeguards); 45 CFR §164.312 (technical safeguards).
[14] 45 CFR §164.530(c)(1).

appropriately safeguard the protected health information they receive or create on behalf of covered entities.[15]

43. The PII and PHI at issue in this case constitutes "protected health information" within the meaning of HIPAA.

44. The HIPAA Security Rule "establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity" or business associate.[16]

45. CAMC inadequately maintained its network security, platform, and software, rendering these easy prey for cybercriminals. In particular its email system was and remains highly vulnerable to phishing attempts.

46. Defendant was on notice that its inadequate data security created a heightened risk of exfiltration, compromise, and theft. Indeed, it had already been sued in connection with a highly similar data breach based on a purported email phishing attack in 2022.

47. Defendant's security failures include:

(a) Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 CFR §164.306(a)(1);

(b) Failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 CFR §164.306(a)(2);

---

[15] 45 CFR §§164.502(e), 164.504(e), 164.532(d)-(e).

[16] U.S. Dep't of Health & Human Services, The Security Rule, https://www.hhs.gov/hipaa/for-professionals/security/index.html (last accessed June 27, 2024).

(c) Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR §164.306(a)(3);

(d) Failing to ensure compliance with HIPAA security standards by Defendant's workforce in violation of 45 CFR §164.306(a)(4);

(e) Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR §164.312(a)(1);

(f) Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 CFR §164.308(a)(1);

(g) Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR §164.308(a)(6)(ii); and

(h) Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 CFR §164.308(a)(5).

48. Simply put, the Data Breach resulted from Defendant's failures to comply with safeguards mandated by HIPAA regulations compounding upon each other.

49. Defendant failed to use reasonable care in maintaining the privacy and security of Plaintiffs' and Class Members' PII and PHI. If Defendant had implemented adequate security measures, cybercriminals could never have accessed the PII and PHI

of Plaintiffs and Class Members, and the Data Breach would have either been prevented in its entirety or have been much smaller in scope. For example, if Defendant had adequately segregated sensitive data, a patient's driver's license, email address, and date of birth number and address would be in a different place from its medical records or insurance records. Likewise, a breach of a single email account should not have allowed a bad actor to access and subsequently attempt to breach sensitive data on more than 67,000 individuals. Under normal circumstances no individual should be able to download even a tiny fraction of that information from the patient database and adequate monitoring should have flagged and stopped the exposed data.

50. Personally Identifiable Information is of high value to criminals. Sensitive information can often be sold on the dark web, with personal information being sold at a price ranging from $40 to $200 and bank details with a price from $50 to $200.[17] The Data Breach exposed PII that is both valuable and highly coveted on underground markets because it can be used to commit identity theft and financial fraud. Identity thieves use such PII to, among other things, gain access to bank accounts, social media accounts, and credit cards. Identity thieves can also use this PII to open new financial accounts, open new utility accounts, obtain medical treatment using victims' health insurance, file fraudulent tax returns, obtain government benefits, obtain government identification cards, or create "synthetic identities." Additionally, identity thieves often wait significant amounts of time—months or even years—to use the PII obtained in data breaches because victims often become less vigilant in monitoring their accounts as time passes, therefore making the PII easier to use without detection.

---

[17] *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, available at: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed February 24, 2025).

51. Victims of data breaches are much more likely to become victims of identity fraud than those who have not. Data Breach victims who do experience identity theft often spend hundreds of hours fixing the damage caused by identity thieves.[18] Plaintiffs and members of the class generally have spent hours on end and considerable time and stress in attempting to mitigate the present and future harms caused by the breach. The U.S. Department of Justice's Bureau of Justice Statistics has reported that, even if data thieves have not caused financial harm, data breach victims "reported spending an average of about 7 hours clearing up the issues."[19]

52. The information compromised in the Data Breach—including names, addresses, dates of birth, Social Security numbers, health insurance plan information, and medical information—is much more valuable than the loss of credit card information in a retailer data breach. There, victims can simply close their credit and debit card accounts and potentially even rely on automatic fraud protection offered by their banks. Here, however, the information compromised is much more difficult, if not impossible, for victims to re-secure after being stolen because it goes to the core of their identity.

53. Data breaches involving medical records are not only incredibly costly, they can "also [be] more difficult to detect, taking almost twice as long as normal identity theft."[20] The FTC warns that a thief may use private medical information to, among other things, "see a doctor, get prescription drugs, buy medical devices, submit

---

[18] https://www.marylandattorneygeneral.gov/ID%20Theft%20Documents/Identitytheft.pdf. (last accessed February 24, 2025)

[19] https://bjs.ojp.gov/content/pub/pdf/vit14.pdf. (last accessed February 24, 2025)

[20] *See What to Know About Medical Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (Last Accessed July 25, 2024).

claims with your insurance provider, or get other medical care"[21] and that this may have far reaching consequences for a victim's ability to access medical care and use insurance benefits.

54. Security standards for businesses storing PII and PHI commonly include, but are not limited to:

a. Maintaining a secure firewall

b. Monitoring for suspicious or unusual traffic on the website

c. Looking for trends in user activity including for unknown or suspicious users

d. Looking at server requests for PII

e. Looking for server requests from VPNs and Tor exit notes

f. Requiring multi-factor authentication before permitting new IP addresses to access user accounts and PII

g. Structuring a system including design and control to limit user access as necessary including a user's access to the account data and PII of other users.

h. Training users in how to spot phishing attempts and enacting safeguards to limit the harm from a single successful phishing attempt.

55. Despite Defendant's statements relating to its obligation to secure patient data, the scale of the breach and the sensitivity of the data indicates Defendant did not use security measures commensurate to its obligations. No single individual should have ever been able to access all the breached information.

---

[21] *Id.*

56. Defendant breached its duty to exercise reasonable care in protecting Plaintiffs' and Class Members' PII and PHI by failing to implement and maintain adequate data security measures to safeguard Plaintiffs' and Class Members' sensitive personal information, failing to encrypt or anonymize PII within its systems and networks, failing to monitor its systems and networks to promptly identify and thwart suspicious activity, failing to delete and purge PII and PHI no longer necessary for its provision of services to its clients, allowing unmonitored and unrestricted access to unsecured PII and PHI, and allowing (or failing to prevent) unauthorized access to, and exfiltration of, Plaintiffs' and Class Members' confidential and private information. Additionally, Defendant breached its duty by utilizing outdated and ineffectual data security measures which deviated from standard industry best practices at the time of the Data Breach. Through these actions, Defendant also violated its duties under the FTC Act and HIPAA.

57. Defendant failed to prevent the Data Breach. Had Defendant properly maintained and adequately protected its systems, servers, and networks, the Data Breach would not have occurred.

V. Plaintiffs' and Class Members' Experiences

58. To use Defendant's healthcare services, Plaintiffs and class members provided sensitive PII and PHI including their full name, address, date of birth, social security number, medical records, insurance information, billing, banking, and credit card information, family medical history, and more. Although it is not clear if additional information was breached, at minimum the breached data included, as discussed above, first and last name; date of birth; email address; phone number; driver's license; health information, and health insurance information.

59. Plaintiff Jedidiah Walls has used Defendant's healthcare services for more than 8 years and takes reasonable precautions to protect his personal data. He received a letter dated February 14, 2025 on or after that date advising him that his personal and health information had been exposed as a result of the data breach. Mr. Walls is a healthcare fraud investigator for the Attorney General's office and is worried and concerned about the implications of this breach with respect to both his access to healthcare services and his credit score.

60. Plaintiff Michael Hill has used Defendant's healthcare services for approximately 30 years and takes reasonable precautions to protect his personal data. He received a letter dated February 14, 2025 on or after that date advising him that his personal and health information had been exposed as a result of the data breach. He is anxious about the data breach and the impact the exposure may have on him and his family.

61. Plaintiff Jennifer Hill has used Defendant's healthcare services for approximately 20 years and takes reasonable precautions to protect her personal data. She received a letter dated February 14, 2025 on or after that date advising her that her personal and health information had been exposed as a result of the data breach. She is anxious about the data breach and the impact the exposure may have on her and her family. She is worried her data has been exposed and will never be able to be recovered. She works for a financial institution and has some knowledge of the kinds of harm that can result from this type of breach.

62. Plaintiffs have taken reasonable steps to maintain the confidentiality of their PII and PHI, and they relied upon Defendant's representations, experience, and sophistication to keep their information secure and confidential.

63. In February 2025 Plaintiffs received data breach notifications from Defendant identifying that their personal information was breached including but not limited to: first and last name; date of birth; email address; phone number; driver's license; health information, and health insurance information.

64. As a result of the data breach, Plaintiffs were forced to take measures to mitigate the harm, including spending time monitoring credit and financial accounts, researching the Data Breach, and researching and taking steps to prevent and mitigate the likelihood of identity theft.

65. As a result of the Data Breach, Plaintiffs are stressed and worried about the impact and will be at continuous and ongoing risk of harm of fraud and identity theft, as well as the loss of the value of their personal information.

66. Plaintiffs and Class Members suffered harm which includes but is not limited to: (a) damages to and diminution in the value of his PII and PHI—property that Plaintiffs and Class Members entrusted to Defendant as a condition of receiving its services; (b) loss and invasion of Plaintiffs' and Class Members' privacy; and (c) injuries arising from the increased risk of fraud and identity theft, including the lost time and cost of taking reasonable identity theft protection measures, which will continue for years.

CLASS ACTION ALLEGATIONS

67. Plaintiffs brings this action as a class action pursuant to Rules 23(a) and 23(b)(1)-(3) of the Federal Rules of Civil Procedure, on behalf of themselves and a Nationwide Class defined as:

All persons in the United States whose PII/PHI was compromised by the Data Breach of CAMC's systems which purportedly occurred between October 2-3, 2024.

68. Excluded from the Nationwide Class are governmental entities, Defendant, any entity in which Defendant have a controlling interest, and Defendant's officers, directors, affiliates, legal representatives, employees, coconspirators, successors, subsidiaries, and assigns. Also excluded from the Nationwide Class are any judges, justices, or judicial officers presiding over this matter and the members of their immediate families and judicial staff.

69. This action is brought and may be properly maintained as a class action pursuant to Rule 23. This action satisfies the requirements of Rule 23, including numerosity, commonality, typicality, adequacy, predominance, and superiority.

70. **Numerosity.** The Nationwide Class is so numerous that the individual joinder of all members is impracticable. While the exact number of Nationwide Class Members is currently unknown and can only be ascertained through appropriate discovery, Plaintiffs, on information and belief, alleges that the Nationwide Class includes at least tens of thousands of individuals based on public reporting.

71. **Commonality.** Common legal and factual questions exist that predominate over any questions affecting only individual Class Members. These common questions, which do not vary among Class Members, and which may be determined without reference to any Class Member's individual circumstances, include, but are not limited to:

a. Whether Defendant knew or should have known that its systems were vulnerable to unauthorized access;

b. Whether Defendant failed to take adequate and reasonable measures to ensure that its data systems were protected;

c. Whether Defendant failed to take available steps to prevent and stop the breach from happening or to mitigate the risk of a long-term breach;

d. Whether Defendant unreasonably delayed in notifying patients of the Data Breach once the suspicious activity was detected.

e. Whether Defendant owed a legal duty to Plaintiffs and Class Members to protect its PII and PHI;

f. Whether Defendant breached any duty to protect the personal information of Plaintiffs and Class Members by failing to exercise due care in protecting their PII and PHI;

g. Whether Plaintiffs and Class Members are entitled to actual, statutory, or other forms of damages and other monetary relief; and,

h. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief or restitution.

72. **Typicality.** Plaintiffs' claims are typical of other Nationwide Class Members' claims because Plaintiffs and Class Members were subjected to the same allegedly unlawful conduct and damaged in the same way.

73. **Adequacy of Representation.** Plaintiffs are adequate class representatives because they are Nationwide Class Members, and their interests do not conflict with the Class interests. Plaintiffs retained counsel who are competent and

experienced in class action and data breach litigation. Plaintiffs and their counsel intend to prosecute this action vigorously for the Class's benefit and will fairly and adequately protect their interests.

74. **Predominance and Superiority.** The Nationwide Class can be properly maintained because the above common questions of law and fact predominate over any questions affecting individual Class Members. A class action is also superior to other available methods for the fair and efficient adjudication of this litigation because individual litigation of each Class member's claim is impracticable. Even if each Class member could afford individual litigation, the court system could not. It would be unduly burdensome if thousands of individual cases proceed. Individual litigation also presents the potential for inconsistent or contradictory judgments, the prospect of a race to the courthouse, and the risk of an inequitable allocation of recovery among those with equally meritorious claims. Individual litigation would increase the expense and delay to all parties and the courts because it requires individual resolution of common legal and factual questions. By contrast, the class-action device presents far fewer management difficulties and provides the benefit of a single adjudication, economies of scale, and comprehensive supervision by a single court.

75. **Declaratory and Injunctive Relief.** The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members that would establish incompatible standards of conduct for Defendant. Such individual actions would create a risk of adjudications that would be dispositive of the interests of other Class Members and impair their interests. Defendant has acted and/or refused to act on grounds

generally applicable to the Class, making final injunctive relief or corresponding declaratory relief appropriate.

CLAIMS FOR RELIEF

Count 1

Negligence

On behalf of Plaintiffs and the Nationwide Class

76. Plaintiffs incorporate by reference and reallege each allegation above as though fully set forth herein.

77. Plaintiffs and Class Members entrusted their PII and PHI with Defendant as a precondition for receiving medical services.

78. Plaintiffs and Class Members entrusted their PII and PHI to Defendant with the understanding that Defendant would safeguard their PII and PHI.

79. Defendant did not take reasonable and appropriate safeguards to protect Plaintiffs and Class Members' PII and PHI.

80. Defendant had full knowledge of the sensitivity of the PII and PHI that they stored and the types of harm that Plaintiffs and Class Members could and would suffer if that PII and PHI were wrongfully disclosed.

81. Defendant promised to take measures to implement and maintain reasonable security procedures and practices.

82. Defendant violated its duty to implement and maintain reasonable security procedures and practices. That duty includes, among other things, designing, maintaining, and testing Defendant's information security controls sufficiently rigorously to ensure that PII and PHI in its possession was adequately secured by, for

example, encrypting sensitive personal information, installing effective intrusion detection systems and monitoring mechanisms, training staff members in how to avoid phishing attacks, using access controls to limit access to sensitive data, regularly testing for security weaknesses and failures, failing to notify patients of the specific breached data in a timely manner, and failing to remedy the continuing harm by unreasonably delaying notifying specific victims who were harmed.

83. Defendant's duty of care arose from, among other things,

a. Defendant's exclusive ability (and Class Members' inability) to ensure that its systems were sufficient to protect against the foreseeable risk that a data breach could occur;

b. Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, failing to adopt reasonable data security measures;

c. Defendant's duty to comply with HIPAA including by implementing reasonable security practices and practices in compliance with the HIPAA Security Rule.

d. Defendant's common law duties to adopt reasonable data security measures to protect patients' PII and PHI and to act as a reasonable and prudent person under the same or similar circumstances would act.

84. Defendant's violation of the FTC Act constitutes negligence per se for purposes of establishing the duty and breach elements of Plaintiffs' negligence claim.

Those statutes were designed to protect a group to which Plaintiffs belong and to prevent the types of harm that resulted from the Data Breach.

85. Defendant had the financial and personnel resources necessary to prevent the Data Breach. Defendant nevertheless failed to adopt reasonable data security measures, in breach of the duties they owed to Plaintiffs and Class Members.

86. Plaintiffs and Class Members were the foreseeable victims of Defendant's inadequate data security. Defendant knew that a breach of its systems could and would cause harm to Plaintiffs and Class Members.

87. Defendant's conduct created a foreseeable risk of harm to Plaintiffs and Class Members. Defendant's conduct included its failure to adequately mitigate harm through negligently failing to inform victims of the breach for more than two months after the purported first discovery of the breach.

88. Defendant knew or should have known of the inherent risks in collecting and storing massive amounts of PII and PHI, the importance of providing adequate data security for that PII and PHI, and the frequent cyberattacks within the medical industry.

89. Defendant, through its actions and inactions, breached its duty owed to Plaintiffs and Class Members by failing to exercise reasonable care in safeguarding its PII and PHI while it was in its possession and control. Defendant breached its duty by, among other things, its failure to adopt reasonable data security practices and its failure to adopt reasonable security and notification practices, including monitoring internal systems and sending notifications to affected victims. Defendant failed to timely notice Plaintiffs and Class Members of suspicious activities and failed to implement sufficiently stringent security measures.

90. Defendant inadequately safeguarded patients' PII and PHI in breach of standard industry rules, regulations, and best practices at the time of the Data Breach.

91. But for Defendant's breach of its duty to adequately protect Class Members' PII and PHI, Class Members' PII and PHI would not have been stolen.

92. There is a temporal and close causal connection between Defendant's failure to implement adequate data security measures and notification practices, the Data Breach, and the harms suffered by Plaintiffs and Class Members.

93. As a result of Defendant's negligence, Plaintiffs and Class Members suffered and will continue to suffer the damages alleged herein.

94. Plaintiffs and Class Members are entitled to all forms of monetary compensation set forth herein, including monetary payments to provide adequate identity protection services. Plaintiffs and Class Members are also entitled to the injunctive relief sought herein.

Count 2

Breach of Implied Contract

On behalf of Plaintiffs and the Nationwide Class

95. Plaintiffs repeat and reallege each and every fact, matter, and allegation set forth above and incorporates them by reference as though set forth in full.

96. Plaintiffs and Class Members entered into an implied contract with Defendant when they entrusted Defendant with their PHI and PII as a precondition for receiving healthcare services.

97. As part of these transactions, Defendant agreed to safeguard and protect the PII and PHI of Plaintiffs and Class Members and to timely and accurately notify them if their PII or PHI was breached or compromised.

98. Plaintiffs and Class Members entered into implied contracts with the reasonable expectation that Defendant's data security practices and policies were reasonable and consistent with legal requirements and industry standards.

99. Plaintiffs and Class Members would not have provided and entrusted their PII and PHI to Defendant in the absence of the implied contract or implied terms between them. The safeguarding of the PII and PHI of Plaintiffs and Class Members was critical to realize the intent of the parties.

100. Plaintiffs and Class members fully performed their obligations under the implied contracts with Defendant.

101. Defendant breached its implied contracts with Plaintiffs and Class Members to protect their PII and PHI when they (1) failed to take reasonable steps to use safe and secure systems to protect that information; (2) disclosed that information to unauthorized third parties and; (3) failed to notify Plaintiffs and Class Members of the specific data breached a reasonably timely manner.

102. As a direct and proximate result of Defendant's breach of implied contract, Plaintiffs and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include ongoing, imminent, certainly impending threat of identity theft crimes, medical identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the

compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of their PII and PHI; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of the Defendant's Data Breach; lost benefit of their bargains and overcharges for services or products; loss of access to medical services and treatment; nominal and general damages; and other economic and non-economic harm.

103. As a direct and proximate result of the breach, Plaintiffs are entitled to relief as set forth herein.

Count 3

Breach of Fiduciary Duty

On behalf of Plaintiffs and the Nationwide Class

104. Plaintiffs repeat and reallege each and every fact, matter, and allegation set forth above and incorporates them by reference as though set forth in full.

105. A relationship existed between Defendant and the Class wherein Plaintiffs and the Class entrusted Defendant with protecting their PII and PHI. Defendant accepted this trust when they accepted the information from Plaintiffs and the class.

106. When Defendant accepted and became guardian of Class Members' personal information, it undertook a fiduciary responsibility to act in the interests of class members with respect to Class Members' PII and PHI. Defendant agreed to

safeguard and protect the PII and PHI of Plaintiffs and Class Members and to timely and accurately notify them if their PII or PHI was breached or compromised.

107. Defendant breached the fiduciary duties that they owed to Plaintiffs and the Class by failing to act with the utmost good faith, fairness, and honesty and failing to act with the highest and finest loyalty.

108. Defendant breached its fiduciary duties by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable period.

109. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to implement reasonable data security practices and policies consistent with legal requirements and industry standards including by failing to encrypt or protect the sufficiency of its systems.

110. Defendant breached its fiduciary duties by failing adequately secure its sensitive data systems, failing to timely notify Plaintiffs and the Class about the data breach, and otherwise failing to safeguard Class Members' PII and PHI.

111. But for Defendant's breach of fiduciary duties, Plaintiffs and class members would not have suffered injured or would have suffered less harm. These injuries include ongoing, imminent, certainly impending threat of identity theft crimes, medical identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other

related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of their PII and PHI; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of the Defendant's Data Breach; lost benefit of their bargains and overcharges for services or products; loss of access to medical services and treatment; nominal and general damages; and other economic and non-economic harm.

112. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class members suffered and continue to suffer the injuries alleged above and other forms of injuries.

113. As a direct and proximate result of Defendant's breach of fiduciary duty, Plaintiffs and the Class are entitled to and demand actual, consequential, and nominal damages and injunctive relief, to be determined at trial.

Count 4

Invasion of Privacy

On behalf of Plaintiffs and the Nationwide Class

114. Plaintiffs, individually and on behalf of the Class, incorporate by reference each of the factual allegations contained in the preceding paragraphs as if fully set forth herein.

115. Plaintiffs and Class Members have a legally protected privacy interest in their PII and PHI, which is and was collected, stored, and maintained by Defendant, and they are entitled to the reasonable and adequate protection of their PII and PHI against foreseeable unauthorized access, as occurred with the Data Breach.

116. Plaintiffs and Class Members reasonably expected that Defendant would protect and secure their PII from unauthorized parties and that their private information would not be accessed, exfiltrated, and disclosed to any unauthorized parties or for any improper purpose.

117. Defendant unlawfully invaded the privacy rights of Plaintiffs and Class Members by engaging in the conduct described above, including by failing to protect their PII and PHI by permitting unauthorized third parties to access, exfiltrate, and view this private information. Likewise, Defendant further invaded the privacy rights of Plaintiffs and Class Members and permitted cybercriminals to invade the privacy rights of Plaintiffs and Class Members, by unreasonably delaying disclosure of the Data Breach and failing to properly identify what PII and PHI had been accessed, exfiltrated, and viewed by unauthorized third parties.

118. This invasion of privacy resulted from Defendant's failure to properly secure and maintain Plaintiffs' and the Members' PII and PHI, leading to the foreseeable unauthorized access, exfiltration, and disclosure of data, including its failure to adequately secure against phishing attacks.

119. Plaintiffs' and the Class Members' PII and PHI is the type of sensitive, personal information that one normally expects will be protected from exposure by the entity charged with safeguarding it. Further, the public has no legitimate concern in Plaintiffs' and the Class Members' PII and PHI, and such private information is otherwise protected from exposure to the public by various statutes, regulations, and other laws.

120. The disclosure of Plaintiffs' and the Class Members' PII and PHI to unauthorized parties is substantial and unreasonable enough to be legally cognizable and is highly offensive to a reasonable person.

121. Defendant's willful and reckless conduct permitted unauthorized access, exfiltration, and disclosure of Plaintiffs' and Class Members' sensitive PII and PHI, causing serious mental injury, shame, embarrassment, or humiliation.

122. The unauthorized access, exfiltration, and disclosure of Plaintiffs' and the Class Members' PII and PHI was without their consent, and in violation of various statutes, regulations, and other laws.

123. As a result of the invasion of privacy caused by Defendant, Plaintiffs and the Class Members suffered and will continue to suffer damages and injury as set forth herein.

124. Plaintiffs and the Class Members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, restitution, injunctive relief, reasonable attorneys' fees and costs, and any other relief that is just and proper.

Count 5

Injunctive/Declaratory Relief

On behalf of Plaintiffs and the Nationwide Class

125. Plaintiffs, individually and on behalf of the Class, incorporate by reference each of the factual allegations contained in the preceding paragraphs as if fully set forth herein.

126. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201 *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties

and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal and state statutes described herein.

127. Defendant owes a duty of care to Plaintiffs and Class Members, which required Defendant to adequately monitor and safeguard Plaintiffs' and Class Members' PII and PHI.

128. Defendant and its officers, directors, affiliates, legal representatives, employees, co-conspirators, successors, subsidiaries, and assigns still possess the PII and PHI belonging to Plaintiffs and Class Members.

129. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and Class Members' PII and PHI and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their PII and PHI. Plaintiffs alleges that Defendant's data security measures remain inadequate. Furthermore, Plaintiffs and the Class continue to suffer injury as a result of the exposure of their PII and PHI and the risk remains that further compromises of their private information will occur in the future.

130. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to secure the PII and PHI of Plaintiffs and the Class within its care, custody, and control under the common law, Section 5 of FTC Act, and HIPAA;

b. Defendant breached its duty to Plaintiffs and the Class by allowing the Data Breach to occur;

c. Defendant's existing data monitoring and phishing protection measures do not comply with its obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect the PII and PHI of Plaintiffs and the Class within Defendant's custody, care, and control; and

d. Defendant's ongoing breaches of said duties continue to cause harm to Plaintiffs and the Class.

131. This Court should also issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with industry standards to protect the PII and PHI of Plaintiffs and the Class within its custody, care, and control, including the following:

a. Order Defendant to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

b. Order that, to comply with Defendant's obligations and duties of care, Defendant must implement and maintain reasonable security and monitoring measures, including, but not limited to:

i. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems, networks, and servers on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

ii. Encrypting and anonymizing the existing PII and PHI within its servers, networks, and systems to the extent practicable, and purging all such information which is no longer reasonably necessary for Defendant to provide adequate services;

iii. Engaging third-party security auditors and internal personnel to run automated security monitoring;

iv. Auditing, testing, and training its security personnel regarding any new or modified procedures;

v. Segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems, networks, and servers;

vi. Conducting regular database scanning and security checks; and

vii. Routinely and continually conducting internal training and education to inform Defendant's internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

132. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach or cybersecurity incident. This risk is real, immediate, and substantial. This is not the first time CAMC has been breached as the result of a phishing attack. If another data breach or cybersecurity incident occurs, Plaintiffs and the Class will not have an adequate remedy at law because monetary relief alone will not compensate Plaintiffs and the Class for the serious risks of future harm.

133. The hardship to Plaintiffs and the Class if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Plaintiffs and the Class will likely be subjected to substantial, continued identity theft and other related damages and or additional data breaches and exposure if an injunction is not issued. On the other hand, the cost of Defendant's compliance with an injunction requiring reasonable

prospective data security measures is relatively minimal, and Defendant has a preexisting legal obligation to employ such measures.

134. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent or larger data breach or cybersecurity incident, thus preventing future injury to Plaintiffs and the Class and other persons whose PII and PHI would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class set forth herein, respectfully request the following relief:

A. That the Court certify this action as a class action and appoint Plaintiffs and their counsel to represent the Class;

B. That the Court grant permanent injunctive relief to prohibit Defendant from continuing to engage in the unlawful acts, omissions, and practices described herein and directing Defendant to adequately safeguard the PII and PHI of Plaintiffs and the Class by implementing improved security controls;

C. That the Court award compensatory, consequential, and general damages, including nominal damages as appropriate, as allowed by law in an amount to be determined at trial;

D. That the Court award statutory or punitive damages as allowed by law in an amount to be determined at trial;

E. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendant as a result of Defendant's unlawful acts, omissions, and practices;

F. That the Court award to Plaintiffs and Class Members the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses; and

G. That the Court award pre- and post-judgment interest at the maximum legal rate and all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demands a jury trial on all claims so triable.

Dated: February 25, 2025

/s/ Christopher T. Pritt

Christopher T. Pritt (WVSBN: 10342)
Chris Pritt Law, PLLC
700 Washington Street, East, Suite 204
Charleston, West Virginia 25301
Phone: 304-720-4412
Email: chris.pritt@prittlaw.com

Amber L. Schubert*
SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St, Ste 200
San Francisco, CA 94123
Tel: (415) 788-4220
Fax: (415) 788-0161
aschubert@sjk.law

Attorneys for Plaintiffs and the Proposed Class

**pro hac vice to be filed*